

September 12, 2018

The Honorable Daniel R. Coats
Director of National Intelligence
Office of the Director of National Intelligence
Washington, DC 20511

Dear Director Coats:

We request that the Intelligence Community report to Congress and the public about the implications of new technologies that allow malicious actors to fabricate audio, video and still images.

Hyper-realistic digital forgeries — popularly referred to as “deep fakes” — use sophisticated machine learning techniques to produce convincing depictions of individuals doing or saying things they never did, without their consent or knowledge. By blurring the line between fact and fiction, deep fake technology could undermine public trust in recorded images and videos as objective depictions of reality.

You have repeatedly raised the alarm about disinformation campaigns in our elections and other efforts to exacerbate political and social divisions in our society to weaken our nation. We are deeply concerned that deep fake technology could soon be deployed by malicious foreign actors.

Forged videos, images or audio could be used to target individuals for blackmail or for other nefarious purposes. Of greater concern for national security, they could also be used by foreign or domestic actors to spread misinformation. As deep fake technology becomes more advanced and more accessible, it could pose a threat to United States public discourse and national security, with broad and concerning implications for offensive active measures campaigns targeting the United States.

Given the significant implications of these technologies and their rapid advancement, we believe that a thorough review by the Intelligence Community is appropriate, including an assessment of possible counter-measures and recommendations to Congress. Therefore, we request that you consult with the heads of the appropriate elements of the Intelligence Community to prepare a report to Congress, including an unclassified version, that includes:

- (a) An assessment of how foreign governments, foreign intelligence services or foreign individuals could use deep fake technology to harm United States national security interests;
- (b) A description of any confirmed or suspected use of deep fake technology by foreign governments or foreign individuals aimed at the United States that has already occurred to date;
- (c) An identification of technological counter-measures that have been or could be developed and deployed by the United States Government or by the private sector to deter and detect the use of deep fakes, as well as analysis of the benefits, limitations and drawbacks, including privacy concerns, of such counter-technologies;

- (d) An identification of the elements of the Intelligence Community that have, or should have, lead responsibility for monitoring the development of, use of and response to deep fake technology;
- (e) Recommendations regarding whether the Intelligence Community requires additional legal authorities or financial resources to address the threat posed by deep fake technology;
- (f) Recommendations to Congress regarding other actions we may take to counter the malicious use of deep fake technologies; and
- (g) Any other information you believe appropriate.

We would appreciate your cooperation in producing this report as soon as feasible, but no later than December 14, 2018. Thank you for your assistance.

Sincerely,

Adam B. Schiff
MEMBER OF CONGRESS

Stephanie Murphy
MEMBER OF CONGRESS

Carlos Curbelo
MEMBER OF CONGRESS